(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102685147 B
(45)授权公告日 2015.04.15

(21)申请号 201210175212.4

(22)申请日 2012.05.31

(73)专利权人 东南大学
地址 210096 江苏省南京市四牌楼 2 号

(72)发明人 宋宇波 朱筱赟 张皓月 谭杭波 王许莲

(74)专利代理机构 南京苏高专利商标事务所（普通合伙） 32204
代理人 柏尚春

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04W 12/00(2009.01)

(56)对比文件
US 2008086776 A1,2008.04.10, 权利要求 1-20,说明书第 [0025]-[0045],[0073]-[0092] 段,图 1-3,11 和 12.
CN 101873556 A,2010.10.27, 全文 .
US 2009144823 A1,2009.06.04, 全文 .

审查员 王瑞

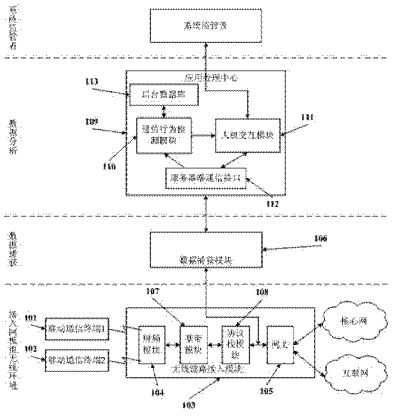
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种移动通信蜜罐捕获系统及其实现方法

(57)摘要

本发明公开了一种移动通信蜜罐捕获系统，包括移动通信终端、无线链路接入模块、数据捕获模块和应用处理中心模块；所述移动通信终端与无线链路接入模块通过无线信道链路进行通信；所述数据捕获模块与应用处理中心模块通过服务器端通信接口模块连接。本发明还公开了一种上述移动通信蜜罐捕获系统的实现方法。本发明不依赖于移动通信终端的硬件设备及系统平台，具有通用性，并且在无线链路上监测通信行为，不占用终端资源。



CN 102685147 B

1. 一种移动通信蜜罐捕获系统，其特征在于：包括移动通信终端、无线链路接入模块、数据捕获模块和应用处理中心模块；

所述移动通信终端与无线链路接入模块通过无线信道链路进行通信；

所述数据捕获模块与应用处理中心模块通过服务器端通信接口模块连接；

所述无线链路接入模块包括射频模块、基带模块、协议栈模块、网关模块，所述射频模块接收空中信号，处理后送入基带模块；发送时从基带模块读出数据进行处理，通过天线发射出去；基带模块主要负责对相关接收数据进行调制、解调；协议栈模块按照移动通信标准对从基带模块接收到的帧进行解析，送至数据捕获模块；发送时广播相应命令，模拟无线接入环境，以控制手机信息被无线链路接入模块捕获；网关模块根据接收到的数据类型，判别接入的网络类型，与真实的通信环境进行交互；

所述数据捕获模块截获协议栈模块和网关模块之间交互的数据，并传送至上层应用处理中心模块；

所述应用处理中心模块包括服务器端通信接口模块、通信行为监测模块、后台数据库模块、人机交互模块；所述服务器端通信接口模块与数据捕获模块连接，实现数据接收和发送控制信息；通信行为监测模块调用服务器端通信接口模块，获得数据捕获模块处理后的数据，对其中的内容进行分析、扫描并与后台数据库比对，检测通信内容中已知的病毒及攻击行为；同时，调用人机交互模块向移动通信终端发送相关数据，通过跟踪、监控、分析其通信行为，发掘新的安全隐患，从而更新、优化后台数据库；后台数据库模块实现恶意行为比对与实时更新功能；人机交互模块调用通信行为监测模块显示监测结果，调用服务器端通信接口模块发送控制信息控制无线链路接入模块，实现告知移动通信终端行为监测结果、协助通信行为监测模块跟踪相关恶意通信行为功能。

2. 一种权利要求 1 所述移动通信蜜罐捕获系统的实现方法，其特征在于：包括以下步骤：

1) 无线链路接入模块初始化，广播含有系统参数的无线电信号，等待移动通信终端连接接入；

2) 移动通信终端初始化，扫描通信网络，根据接收到的信号参数，对其发送连接请求，做好接入准备；

3) 无线链路接入模块对自身环境进行配置管理，向移动通信终端发送信号，允许接入，并为其分配相关通信资源；

4) 通信连接成功建立后，移动通信终端向无线链路接入模块上报数据；

5) 无线链路接入模块对接收的原始通信数据，进行网络协议解析的操作，以模拟真实的无线环境，实现信息交互；

6) 数据捕获模块截获无线链路接入模块中协议栈子模块与网关子模块间交互的数据，对其进行处理并形成可执行的文件，传送至应用处理中心模块；

7) 应用处理中心模块中的通信行为监测模块根据接收到的文件信息，综合利用后台数据库数据，进行通信行为监测，同时将新的恶意行为进行添加到数据库；

8) 该捕获系统的监管者可以通过人机交互模块随时获知移动通信终端的系统安全状态并告知移动通信终端监测结果，实现无线链路层的安全防护功能。

一种移动通信蜜罐捕获系统及其实现方法

技术领域

[0001] 本发明属于无线网络技术领域，涉及一种蜜罐捕获系统及其实现方法，具体是一种模拟无线接入环境针对移动终端通信行为进行监测的蜜罐捕获系统及其实现方法。

背景技术

[0002] 当今世界，移动通信技术迅猛发展，其优越性贯穿生活的方方面面。在它给我们带来方便的同时，也对用户的安全通信造成了威胁。伴随着智能手机的普及，其高效的多任务切换及无线上网功能深受人们喜爱，但不可避免地，遭受病毒攻击的可能性也大大提高。针对这一现象，有人提出了终端防护、核心网架设、基于基站的手机防护等解决方案。之于终端防护的解决方案，现今市场上虽然有针对手机病毒的安全防护软件，但因其都根植于一定的硬件设备，所以灵活性较低、资源占用率大；因其很难满足多样化的手机系统，通用性差，所以市场前景有待考量；因其缺乏无线链路的安全防护功能，所以病毒截获率低。之于核心网架设的方案，核心网相关网源设备布局困难、成本高的特点使该方案存在局限性。之于基于基站的手机防护的方案，基站灵活性差，便携性低，也使该方案存在不足。

[0003] 网络安全防护中采用的蜜罐技术为移动通信安全防护提供了新的思路。蜜罐技术原是一种可被黑客探测、攻击甚至被攻破而泄密的安全资源。它通过诱使黑客入侵，进而收集证据并对黑客的攻击行为进行分析，在隐藏真实的服务器地址的前提下，实施安全防护。

[0004] 诚然，针对移动通信的信息安全问题一直难以得到彻底解决，由此大大影响了手机用户的通信保障。本发明提出的模拟无线接入环境进行移动终端行为监测的移动通信蜜罐捕获系统可以很好解决这个问题。本发明以蜜罐技术为基础，将该技术运用于无线链路上，针对移动终端的通信行为进行监测、分析，发掘安全隐患，优化防护环境。同时，该装置布局简单、易于实施，于未来必能大大减少信息窃取、流失等安全问题，并在商业活动合理开展、个人信息安全防护等方面起到举足轻重的作用。

发明内容

[0005] 本发明的目的在于提供一种移动通信蜜罐捕获系统，是一种模拟无线接入环境针对移动终端通信行为进行监测的方法，以此来有效发掘安全隐患，优化防护环境，从而大大提高系统安全防护能力，克服移动通信中现有的安全防护措施病毒截获率低、灵活性差等缺点。

[0006] 本发明的另一个目的在于提供一种移动通信蜜罐捕获系统的实现方法。

[0007] 本发明采用的技术方案是：一种移动通信蜜罐捕获系统，包括移动通信终端、无线链路接入模块、数据捕获模块和应用处理中心模块；

[0008] 所述移动通信终端与无线链路接入模块通过无线信道链路进行通信；

[0009] 所述数据捕获模块与应用处理中心模块通过服务器端通信接口模块连接。

[0010] 作为优选，所述无线链路接入模块包括射频模块、基带模块、协议栈模块、网关模块，所述射频模块接收空中信号，处理后送入基带模块；发送时从基带模块读出数据进行处

理，通过天线发射出去；基带模块主要负责对相关接收数据进行调制、解调；协议栈模块按照移动通信标准对从基带模块接收到的帧进行解析，送至数据捕获模块；发送时广播相应命令，模拟无线接入环境，以控制手机信息被无线链路接入模块捕获；网关模块根据接收到的数据类型，判别接入的网络类型，与真实的通信环境进行交互。

[0011] 该无线链路接入模块主要负责在无线环境下搭建接入网络，模拟真实基站的接入环境，诱使手机与之通信，捕获相关数据。无线链路接入模块可以是一个或多个，与所要捕获的信号范围相关。

[0012] 作为优选，所述数据捕获模块截获协议栈模块和网关模块之间交互的数据，并传送至上层应用处理中心模块。

[0013] 该数据捕获模块完成了无线链路接入模块与应用处理中心模块间的衔接工作。

[0014] 作为优选，所述应用处理中心模块包括服务器端通信接口模块、通信行为监测模块、后台数据库模块、人机交互模块；所述服务器端通信接口模块与数据捕获模块连接，实现数据接收和发送控制信息；通信行为监测模块调用服务器端通信接口模块，获得数据捕获模块处理后的数据，对其中的内容进行分析、扫描并与后台数据库比对，检测通信内容中已知的病毒及攻击行为；同时，调用人机交互模块向移动终端发送相关数据，通过跟踪、监控、分析其通信行为，发掘新的安全隐患，从而更新、优化后台数据库；后台数据库模块实现恶意行为比对与实时更新功能；人机交互模块调用通信行为监测模块显示监测结果，调用服务器端通信接口模块发送控制信息控制无线链路接入模块，实现告知移动通信终端行为监测结果、协助行为监测模块跟踪相关恶意通信行为功能。

[0015] 上述移动通信蜜罐捕获系统的实现方法，包括以下步骤：

[0016] 1）无线链路接入模块初始化，广播含有系统参数的无线电信号，等待移动通信终端连接接入；

[0017] 2）移动通信终端初始化，扫描通信网络，根据接收到的信号参数，对其发送连接请求，做好接入准备；

[0018] 3）无线链路接入模块对自身环境进行配置管理，向移动通信终端发送信号，允许接入，并为其分配相关通信资源；

[0019] 4）通信连接成功建立后，移动终端向无线链路接入模块上报数据；

[0020] 5）无线链路接入模块对接收的原始通信数据，进行网络协议解析等一系列操作，以模拟真实的无线环境，实现信息交互；

[0021] 6）数据捕获模块截获无线链路接入模块中协议栈子模块与网关子模块间交互的数据，对其进行处理并形成可执行的文件，传送至应用处理中心模块；

[0022] 7）处理中心模块中的通信行为监测模块根据接收到的文件信息，综合利用后台数据库数据，进行通信行为监测，同时将新的恶意行为进行添加到数据库；

[0023] 8）该监测系统的监管者可以通过人机交互模块随时获知移动终端的系统安全状态并告知移动终端监测结果，实现无线链路层的安全防护功能。

[0024] 有益效果：本发明通过广播无线电信号，模拟无线接入环境，诱使移动通信终端接入监测装置，经过处理后在无线链路层进行恶意通信行为的监测、分析与记录。在移动终端进行通信的过程中，无论病毒存在与否，信息的传送一定要经过无线链路，本发明充分利用这一特点，同时结合蜜罐技术的思想，将蜜罐捕获系统应用于无线链路，发掘安全隐患，优

化防护环境，从而大大提高系统安全防护能力。现有的安全防护系统均需根植于某个固定平台，而本发明的安全防护过程是在无线链路而非移动通信终端进行，摆脱了特定平台的束缚，从而减轻了移动终端的负荷，降低资源占用率，减少了人力物力的消耗，加强了通用性。此外，本发明布局简单、易于实施、成本低、灵活性高。

附图说明

[0025] 图 1 为本发明的移动通信蜜罐捕获装置的工作原理示意图；

[0026] 其中有：第一移动通信终端 101、第二移动通信终端 102，无线链路接入模块 103，射频前端模块 104，基带模块 105，协议栈模块 106，网关模块 107，数据捕获模块 108，应用处理中心模块 109，通信行为监测模块 110，人机交互模块 111，服务器端通信接口 112，后台数据库模块 113。

[0027] 图 2 为本发明的移动通信蜜罐捕获方法示意流程图。

具体实施方式

[0028] 下面结合附图和具体实施方式对本发明作进一步说明：

[0029] 如图 1 所示，本蜜罐捕获系统包含一个无线链路接入模块 103 放置在第一移动通信终端 101、第二移动通信终端 102 (即通过无线网络接入基站的用户)附近，模拟无线环境下的真实通信过程。数据捕获模块 108 拦截到短信和通用分组无线业务 (GPRS, General Packet Radio Service) 数据之后通过有线信道把数据传输到应用处理中心 109。这样实现在通信网络内部截取数据，然后将数据发至应用处理中心进行进一步处理，最终实现通信行为的监测。

[0030] 本发明的无线链路接入模块 103 是嵌入式设备，其组件射频模块 104、基带模块 105 在 FPGA 平台上实现，协议栈模块 106、网关模块 107 在 X86 平台上运行。它的作用是放置在第一移动通信终端 101 或第二移动通信终端 102 附近，模拟无线接入环境，由射频前端 104 捕捉通过无线链路接入基站的通信数据，处理后送入基带模块 105 进行解调，并将解调后的帧送给 X86 平台；发送时从基带模块 105 读出调制后的数据进行处理，通过天线发射出去。协议栈模块 106 对接收到的帧进行信令分析，得到国际移动用户识别码 (IMSI, International Mobile Subscriber Identity) 号及通信内容；发送时向手机广播不同命令，以控制手机是否接入无线链路接入模块 103。网关模块 107 主要负责根据接收到的数据类型，判别接入的网络为全球移动通信系统 (GSM , Global System for Mobile Communications) 核心网还是互联网，与真实的通信环境进行交互。其中第一移动通信终端 101、第二移动通信终端 102 不一定都要在同一个无线链路接入模块 103 的覆盖范围内，只要有一个在无线链路接入模块 103 附近即可对其覆盖范围下的移动终端进行诱使接入。

[0031] 应用处理中心模块 109 通过服务器通信端口 112 接收到捕获的解析数据后，进行通信行为监测，并与后台数据库 113 进行比对，检测通信内容中已知的病毒及攻击行为。另外，在检测过程中通过数据交互发掘新的安全隐患，从而更新、优化后台数据库。同时该检测系统的监管者可以通过人机交互模块随时获知移动终端的系统安全状态并告知移动终端行为监测结果，实现无线链路层的安全防护功能。

[0032] 如图 2 所示，本发明的具体工作流程包括以下步骤：

[0033] 步骤 201 :无线链路接入模块进行初始化,等待移动通信终端连接接入,此时移动通信终端已经被安放在无线链路接入模块所覆盖的网络内 ;

[0034] 步骤 202 :移动通信终端初始化并检测网络信号,接受网络内的广播信号,根据获得的信号强弱,确定无线链路接入模块,主动向其发送连接请求,允许后与无线链路接入模块建立无线链路连接,双方实现正常通信。

[0035] 步骤 203 :所述接入模块在无线环境下搭建接入网络,该模块中的协议栈对接收原始的通信数据,进行网络协议解析等一系列操作,以模拟真实的无线环境,实现信息交互 ;

[0036] 这里,所述协议栈可以是 GSM 协议栈或 GPRS 协议栈。

[0037] 步骤 204 :数据捕获模块截获无线链路接入模块中协议栈子模块与网关子模块间交互的数据,对其进行处理并形成可执行的文件,传送至应用处理中心模块 ;

[0038] 步骤 205 :上层应用处理中心通过服务器终端通信接口接收上传的数据。这里,所述数据可以是短信内容或 GPRS 数据。

[0039] 步骤 206 ～ 207 :应用处理中心模块中的通信行为监测模块根据接收到的文件信息,对其中的内容进行分析、扫描并与后台数据库比对,检测通信内容中已知的病毒及攻击行为 ;同时,调用人机交互模块向移动终端发送相关数据,通过跟踪、监控、分析其通信行为,发掘新的安全隐患,并更新、优化后台数据库。

[0040] 步骤 208 :该蜜罐捕获系统的监管者通过 x86 平台上的人机交互模块随时获知移动终端的系统安全状态并告知移动终端行为监测结果,实现无线链路层的安全防护功能。

[0041] 应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。本实施例中未明确的各组成部分均可用现有技术加以实现。

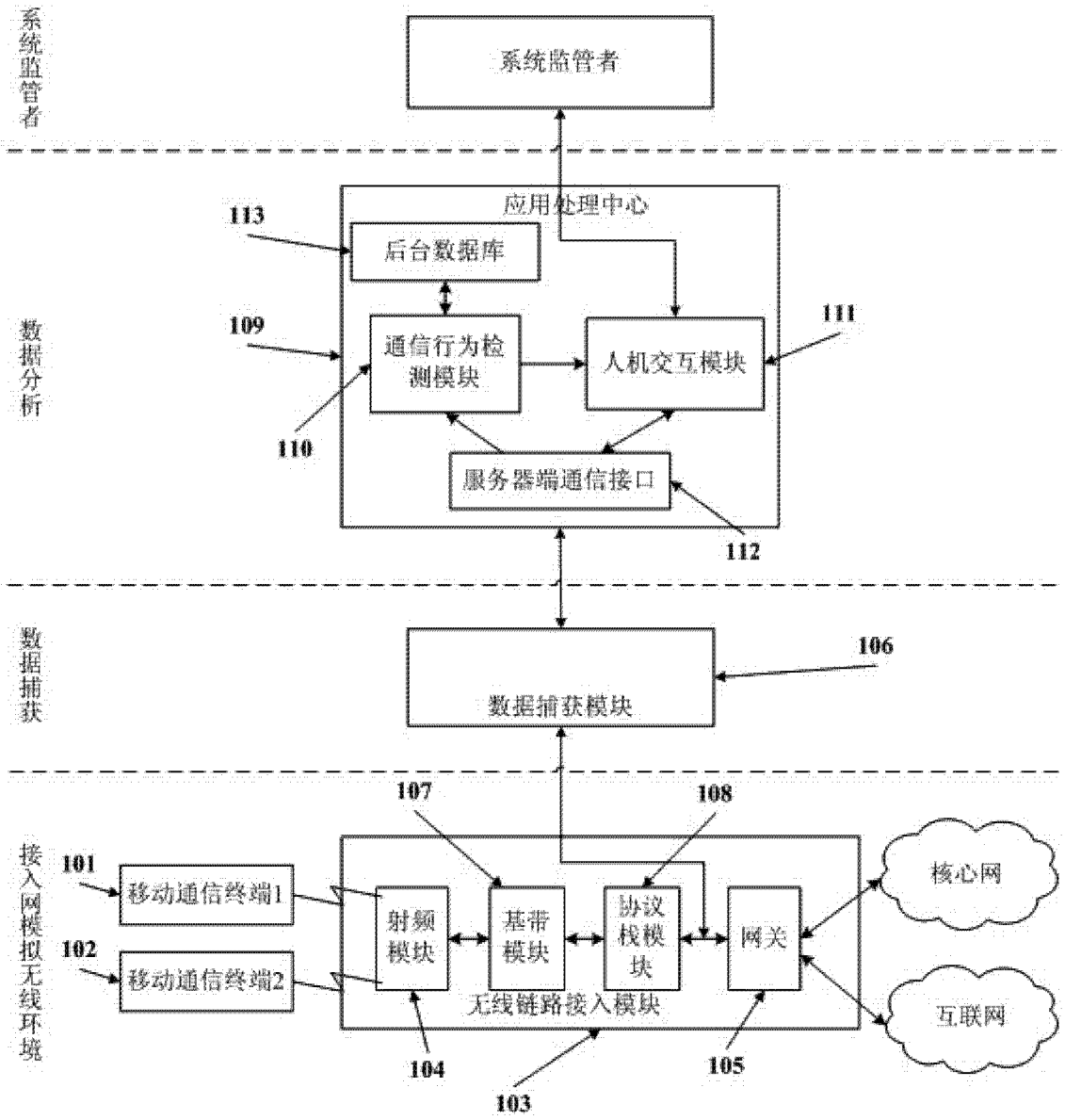

系统监管者
系统监管者
数据分析
应用处理中心
113
后台数据库
109
通信行为检测模块
111
人机交互模块
110
服务器端通信接口
112
数据捕获
106
数据捕获模块
107
108
接入网模拟无线环境
101
移动通信终端1
102
移动通信终端2
射频模块
基带模块
协议栈模块
网关
无线链路接入模块
核心网
互联网
104
103
105

图 1

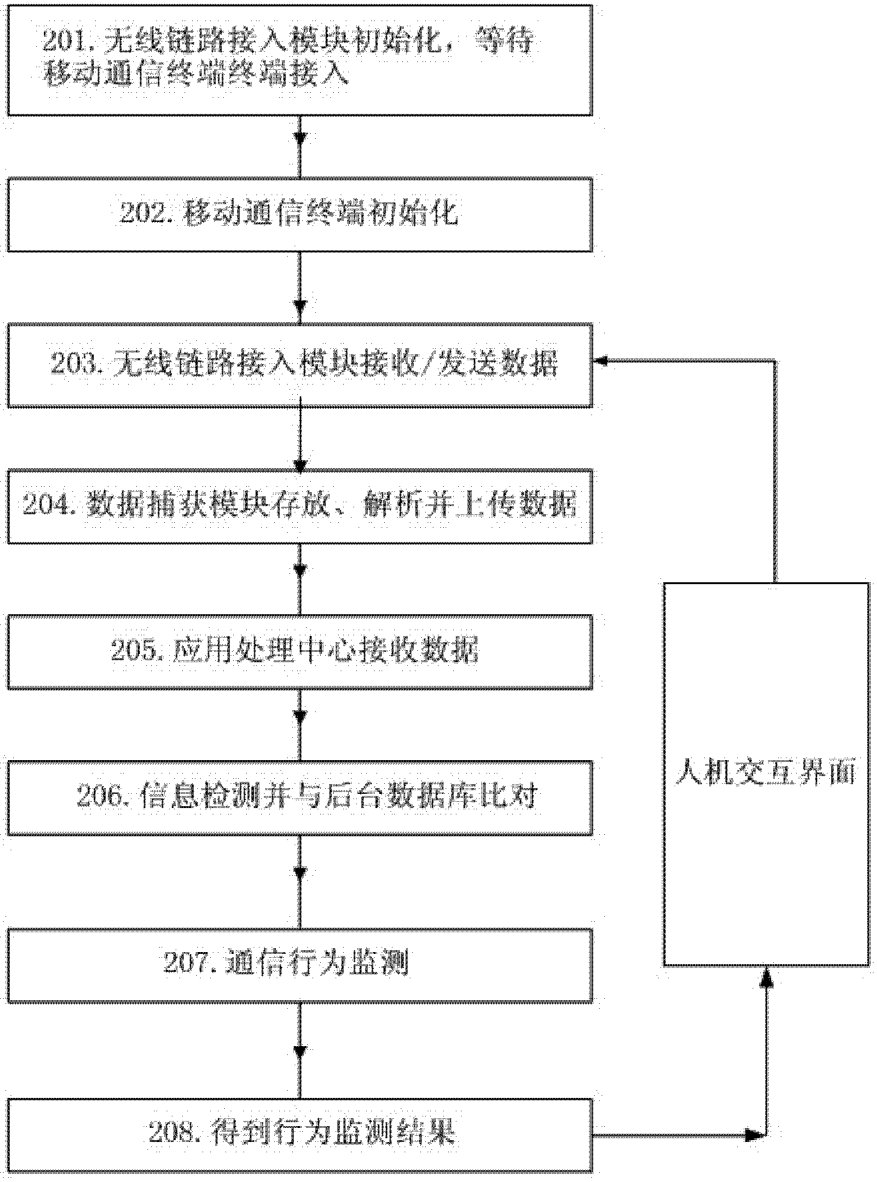

201. 无线链路接入模块初始化，等待移动通信终端终端接入
202. 移动通信终端初始化
203. 无线链路接入模块接收/发送数据
204. 数据捕获模块存放、解析并上传数据
205. 应用处理中心接收数据
206. 信息检测并与后台数据库比对
207. 通信行为监测
208. 得到行为监测结果
人机交互界面

图 2